Cryptology ePrint Archive: Report 2011/355

On the (Non-) Equivalence of UC Security Notions

Oana Ciobotaru

Abstract: In this work we investigate the relations among various security notions and show their connection with the game-theoretic notion of strong universal implementation. More precisely, we present a separation result between two variants of UC security definition: 1-bit specialized simulator UC security and specialized simulator UC security. This solves an open question from [Lindell03] and comes in contrast with the well known equivalence result between 1-bit UC security and UC security. We also give a notion of weak security and we show that the induced weak security under 1-bounded concurrent general composition is equivalent to 1-bit specialized simulator UC security. As a consequence, we obtain that our notion of weak security and the notion of stand-alone security are not equivalent.

By comparing our notion of weak security to a variant of strong universal implementation, we are able to answer positively the open question from [Halpern,Pass10] regarding the existence of game-theoretic notions that are equivalent to cryptographic security definitions with (more) standard order of quantifiers.

In order to achieve the separation result, we employ time-lock puzzles from which we derive a result interesting also on its own, mainly a construction of a one-way function and a hard-core predicate.

Category / Keywords: weak security;1-bit specialized simulator UC security; time-lock puzzles; game theory

Date: received 1 Jul 2011, last revised 24 Oct 2011

Contact author: ociobota at mpi-inf mpg de

Note: This version of the paper has a more detailed proof of the separation result between 1-bit specialized simulator UC security and specialized simulator UC security. This includes an interesting result on its own, mainly a construction of a one-way function from time-lock puzzles.

A new section has been added for proving the equivalence between our notion of weak security and the game theoretic notion of strong universal implementation.

Version: 20111024:155225 (All versions of this report)